DISCIPLINE: Network Communications Protection

Discipline Roadmap for: IPS (Intrusion Prevention System) / IDS (Intrusion Detection System)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Perimeter Juniper → Cisco → SourceFire / Nortel → McAfee → 3Com → SonicWALL →		Market Watch of IPS / IDS merged within multifunctional security device, e.g. a firewall, security device.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Juniper, Cisco, SourceFire / Nortel, McAfee, 3Com, SonicWall

Containment Targets

N/A

Emerging Platforms

IPS / IDS merged w/in multifunctional security device, e.g. a firewall, security device.

Implications and Dependencies

- Costs and implementation considerations can be substantial (~$30-$150k).
- SNMP v3

Roadmap Notes

- IDS still valid for asynchronous forensics.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Network Communications Protection

Discipline Roadmap for: IPS (Intrusion Prevention System) / IDS (Intrusion Detection System)

- **Discipline Boundaries:**
  - An IPS is any device which exercises control to protect networks, applications and computers from exploitation. IPS are intended to resolve ambiguities in passive network monitoring by placing detection in-line. There are 4 basic types of IPS: host-based (addressed in its own roadmap), network, content-based, and rate-based. Network IPS (NIPS) are designed to inspect traffic and can drop malicious traffic. Content-based IPS are designed to inspect network packets and can avoid infections and hacks. Rate-based IPS are designed to prevent denial of services attacks.
  - An IDS is a device which is used to detect all types of malicious network traffic and computer usage that can't be detected by conventional firewalls. An IDS differs from an IPS mainly in that it requires much more human involvement and is implemented near-line instead of in-line.
- **Discipline Standards:**
  - Currently, there are no IPS or IDS specific standards.
- **Migration Considerations:**
  - The biggest problem with IPS/IDS is false reports, either false positives (alerts w/o validity) or false negatives (no alerts when actual threats exist). Both problems are typically due to tuning issues, under or over tuning respectively. Because neither system can completely avoid false reports, it is recommended that tuning err towards false negatives, given the inherently greater consequences.
  - IDS tends to have higher manpower costs, while IPS tends to have functionality risks.
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007